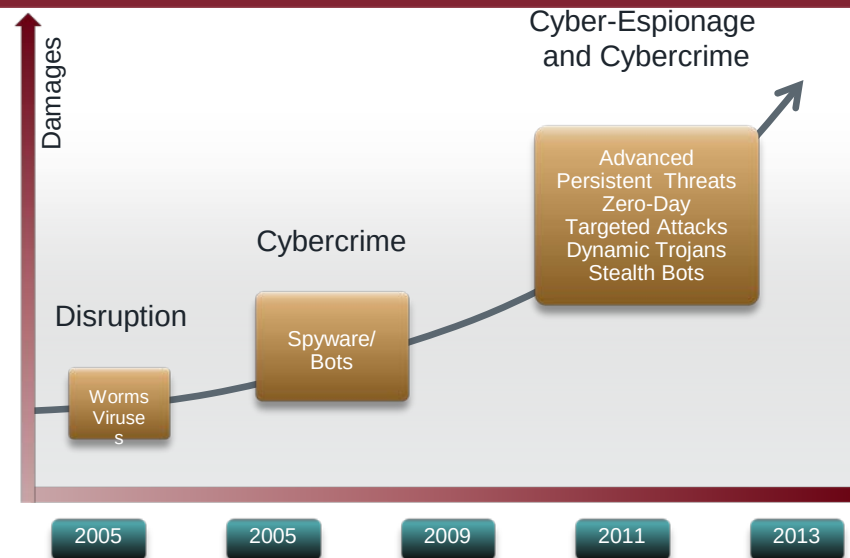




Mitigating APT: The Human Way

Rohyt Belani
Co-founder & CEO
PhishMe, Inc.

Nature of Advanced Cyber Attacks



Evolving cyber
actors

Changing cyber
attacks

Shrinking barriers to
entry

New Threat Landscape

A Report From The Trenches

How a Phishing Attack Exposed an Energy Company to Hackers

By: Brian Prince

2009-09-08

Article Rating: ★★★★★ / 6



Share This Article



[There are 3 user comments on this Security story.](#)

The Intrepidus Group reveals some details behind a malware attack that exposed critical systems at an energy company. Using a Microsoft zero-day vulnerability and a bit of social engineering, hackers compromised a workstation and threatened critical SCADA systems, the security vendor says.

Symptoms

- Windows Security Event ID: 624 on Domain Controller (DC)

New Account Name: backupsrvss

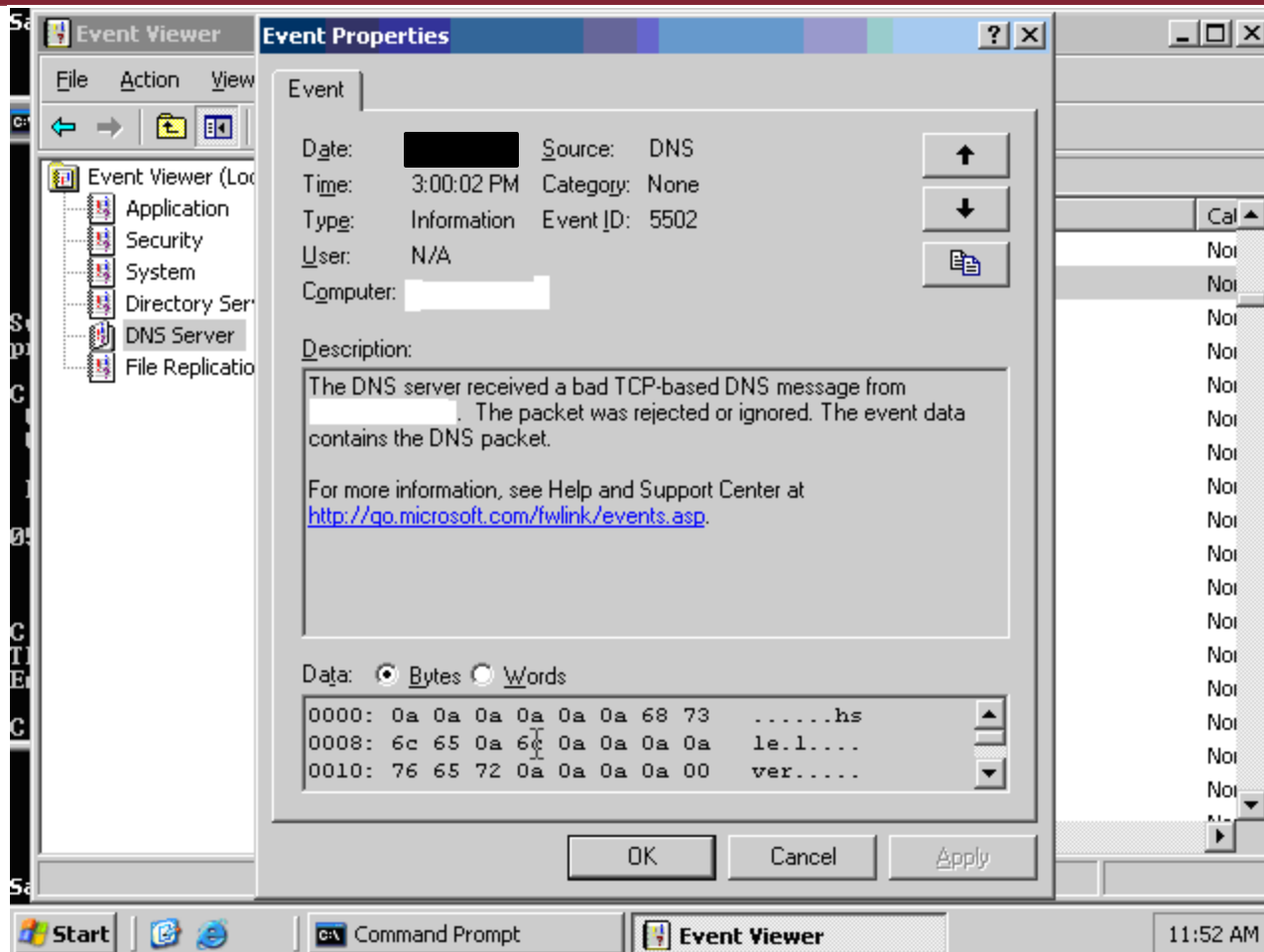
Caller User Name: SYSTEM

Privileges: administrator

Preliminary Investigation

- Windows Security Event Log ID: 540 with a time stamp of (T+3) hours
- Username: ABCDOMAIN \ ABCADMIN
- Logon Type: 3 indicated Network Logon
- Source Network Address indicated that the logon originated from a workstation (\\RIVER) in the most guarded part of the network

That's How the DC fell...



Honing In On RIVER

Live Response

- Smart Card Manager service associated with `ipripsvc.dll`
- An analysis of the DLL indicated that it was similar to Backdoor.Ripgof.B

Honing In On RIVER

- Email & web browsing activity review
 - Request to “/images/singup.exe” from a site in Taiwan @ T-7 days
 - Email from the organization’s HR department on (T-7 days) with an attachment called “Healthcare_Update.chm”

Case Conclusion

- Internet recon used to identify target
 - Employee with 3 kids -> lower healthcare premium is appealing
 - Job profile indicated potential access to SCADA controllers
- Spear phishing email containing “malicious” attachment sent
- Opening the attachment installed the backdoor; foothold gained
- Attackers escalate privileges
- Fortunately, no catastrophic consequences

Some Statistics

135,000
SPEAR PHISHING
EMAILS SENT

80
companies
targeted

28,000
IP addresses used to
send emails

**20 “LEGITIMATE”
WEB SITES
HIJACKED TO
HOST MALWARE**

80 DAYS TO
DISCOVER
MALICIOUS
BREACHES

91 percent of
cyberattacks
that begin with
spear phishing

123 days to
resolve
malicious
breaches

\$8,900,000
AVERAGE ANNUAL COST OF CYBER CRIME

\$222
COST PER
COMPROMISED RECORD

3.9x
higher cost of
cyber crime if
under protected

- Massive-scale phishing attacks loom as new threat, USA Today
- Ponemon Institute: 2012 Cost of Cyber Crime Study
- 2012 Verizon Data Breach Investigations Report
- 'Spear phishing' the main email attachment threat, ComputerWorld UK

..and technical controls are failing

Did these companies
not have the best
defensive and
detective technologies
in place?

أرامكو السعودية
Saudi Aramco



THE WALL STREET JOURNAL.

Human Mitigation

“The reason attackers are able to successfully exploit the security gap is that **they are targeting people**, not computer systems”
– Kevin Mandia, CEO, Mandiant

“If you're being attacked by an intelligent human, your **most useful defense is to also be an intelligent human.**”
– Bruce Schneier

“Security is not a technology issue – **it's a people issue**”
– Steve Mansfield-Devine, ContraRISK

We need to change the way we defend



“But security awareness doesn’t work”

It didn’t, because we were:

- Boring
- De-focused
- Compliance oriented
- Passive

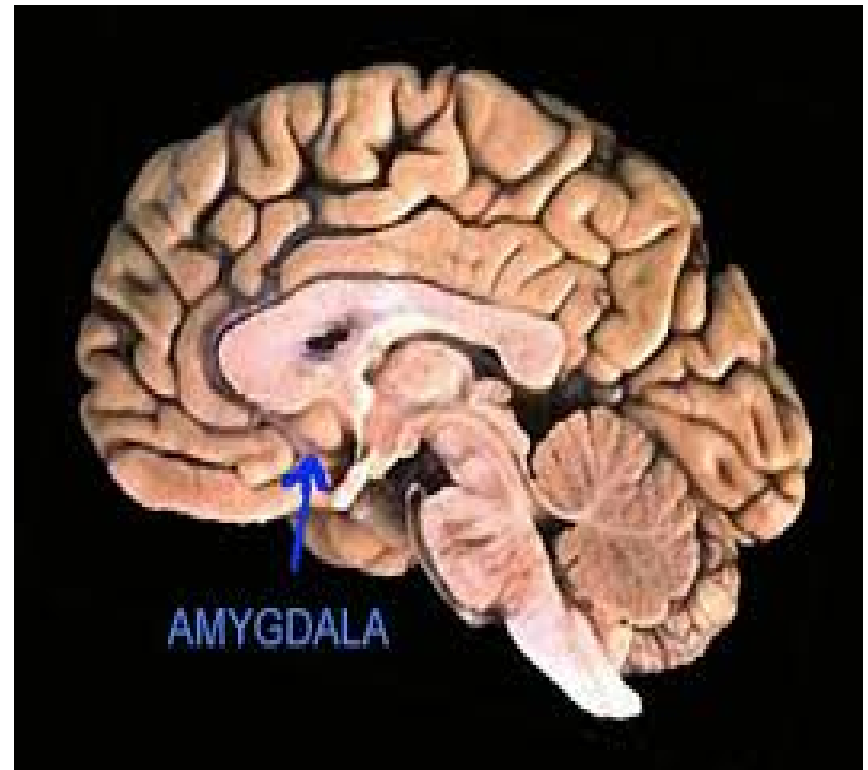
and..

We didn’t have metrics to prove otherwise



Understanding the H_u Element

Memories associated with emotional events are stored here



Learning Theory

- For memories to last, we need long term potentiation (LTP)
- LTP – “ long-lasting enhancement in signal transmission between two neurons that results from stimulating them synchronously”
- Persistence or repetition of an activity tends to induce lasting cellular changes that add to stability in signal transmission between neurons

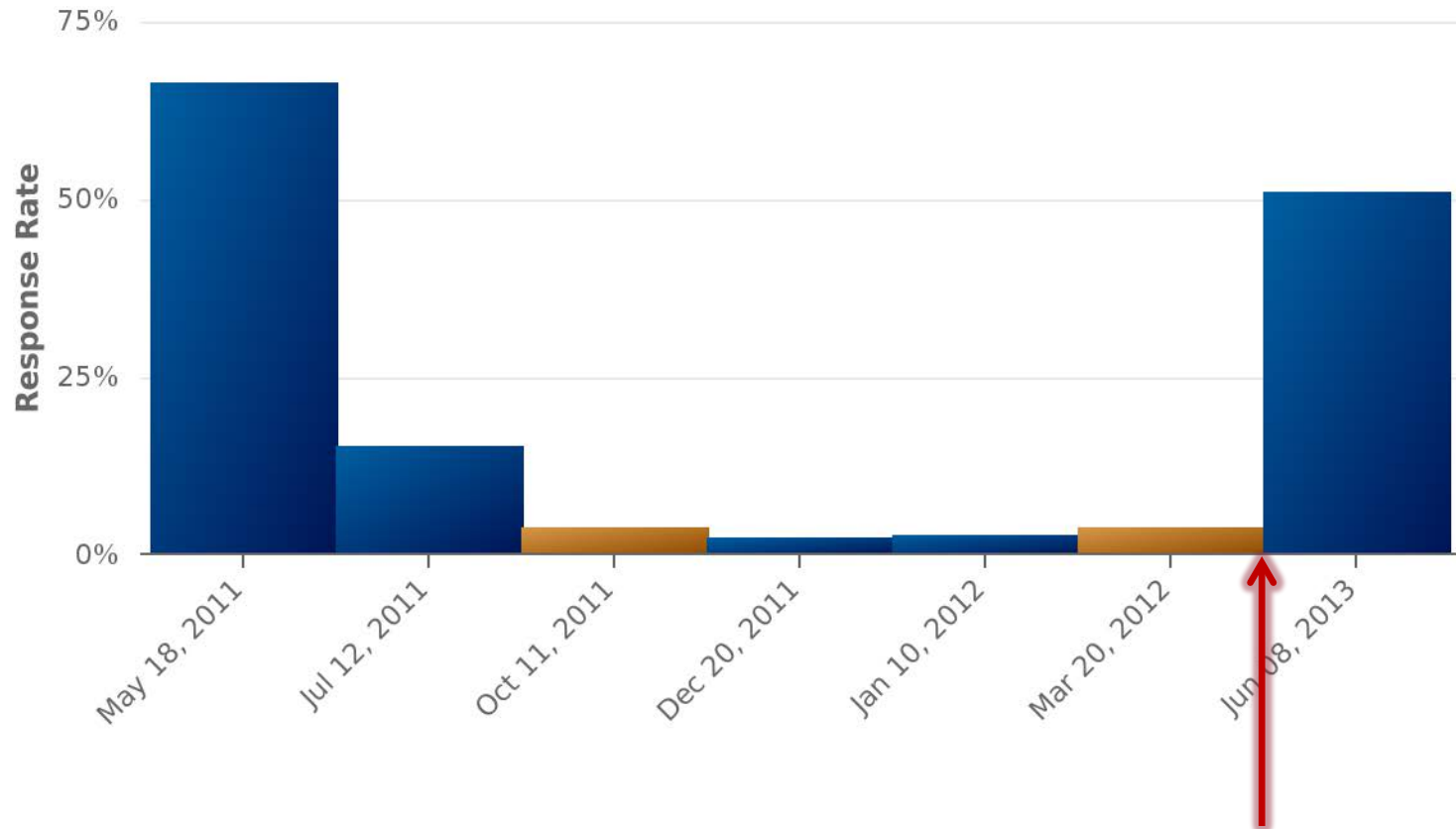


Human Psyche Hacked

- To change behavior, we need:
 - Emotional triggers
 - Repetition
 - Feedback loops
 - Focused information
 - Develop intuition



Making It Work: It Needs to be Continuous



What happened here?

Making It Work: Focus on the Real Threats

Before you spend time and money on training ask yourself – can I fix this issue with a technical control?

Example,
Password complexity – do I really need my users to know what makes a strong password?

USB sticks – can't I just disable them?



Making It Work: Think “Marketing”

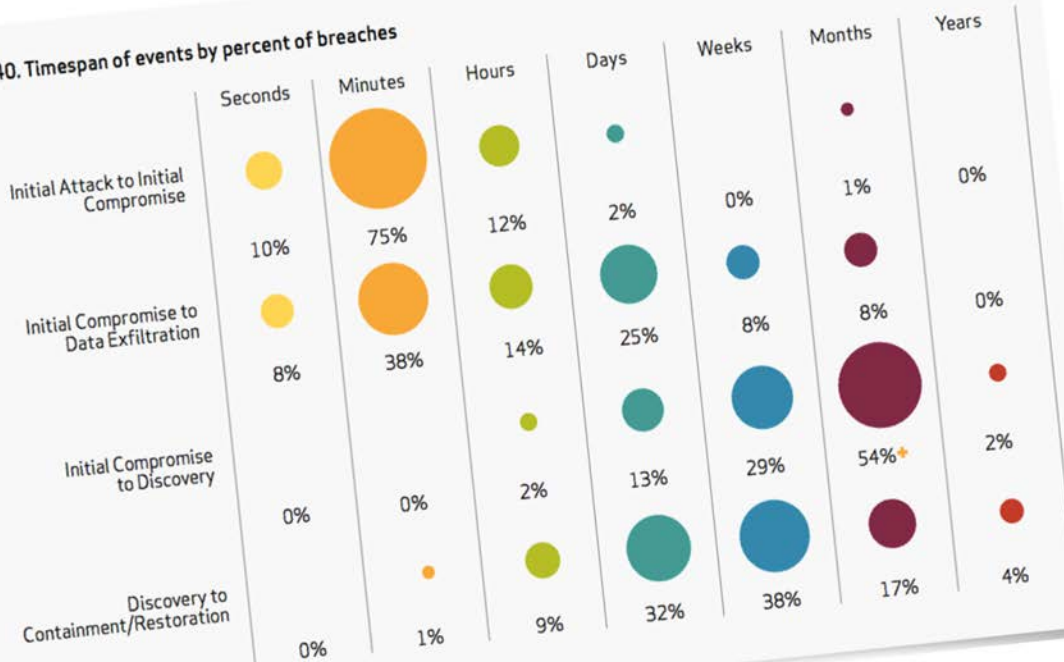


Making It Work: Immerse in the Experience



Knives At A Gunfight

Figure 40. Timespan of events by percent of breaches



Time from compromise
to exfiltration:
Minutes - Days

Time from compromise
to discovery:
Days - Months

Time from discovery to
containment:
Days - Months

Effective threat protection demands discovery in minutes, not months

We Have a Detection Problem!

- Median number of days that attackers were present on a victim network before detection?

243¹

- Percentage of breaches that went undetected for “months or more”?

66%²

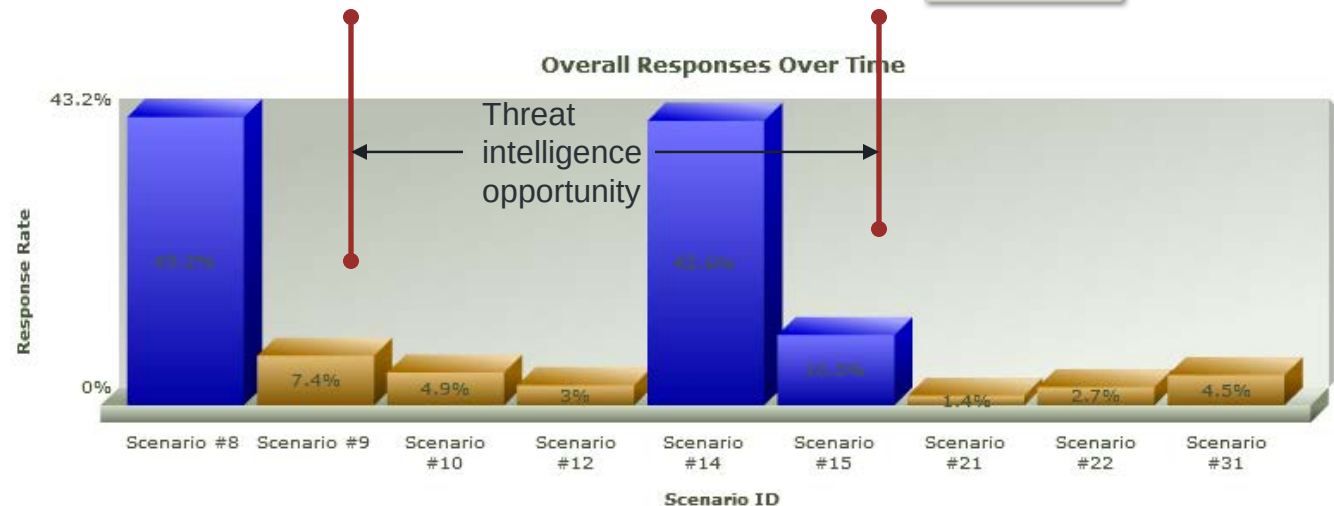
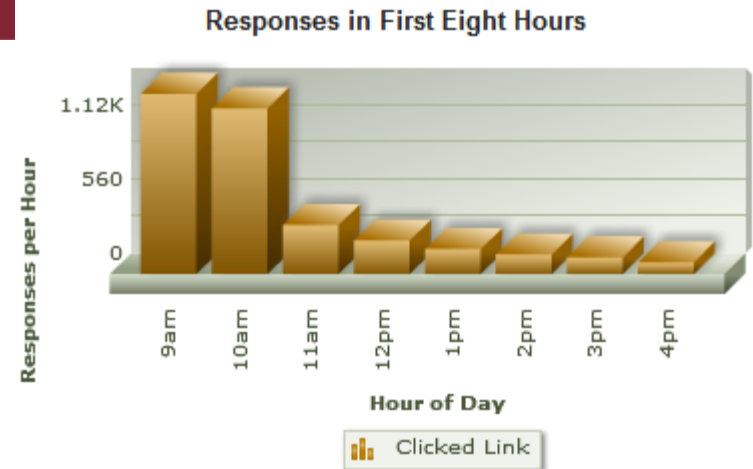
1 www.mandiant.com/library/M-Trends_2013.pdf

2 <http://www.verizonenterprise.com/DBIR/2013/>

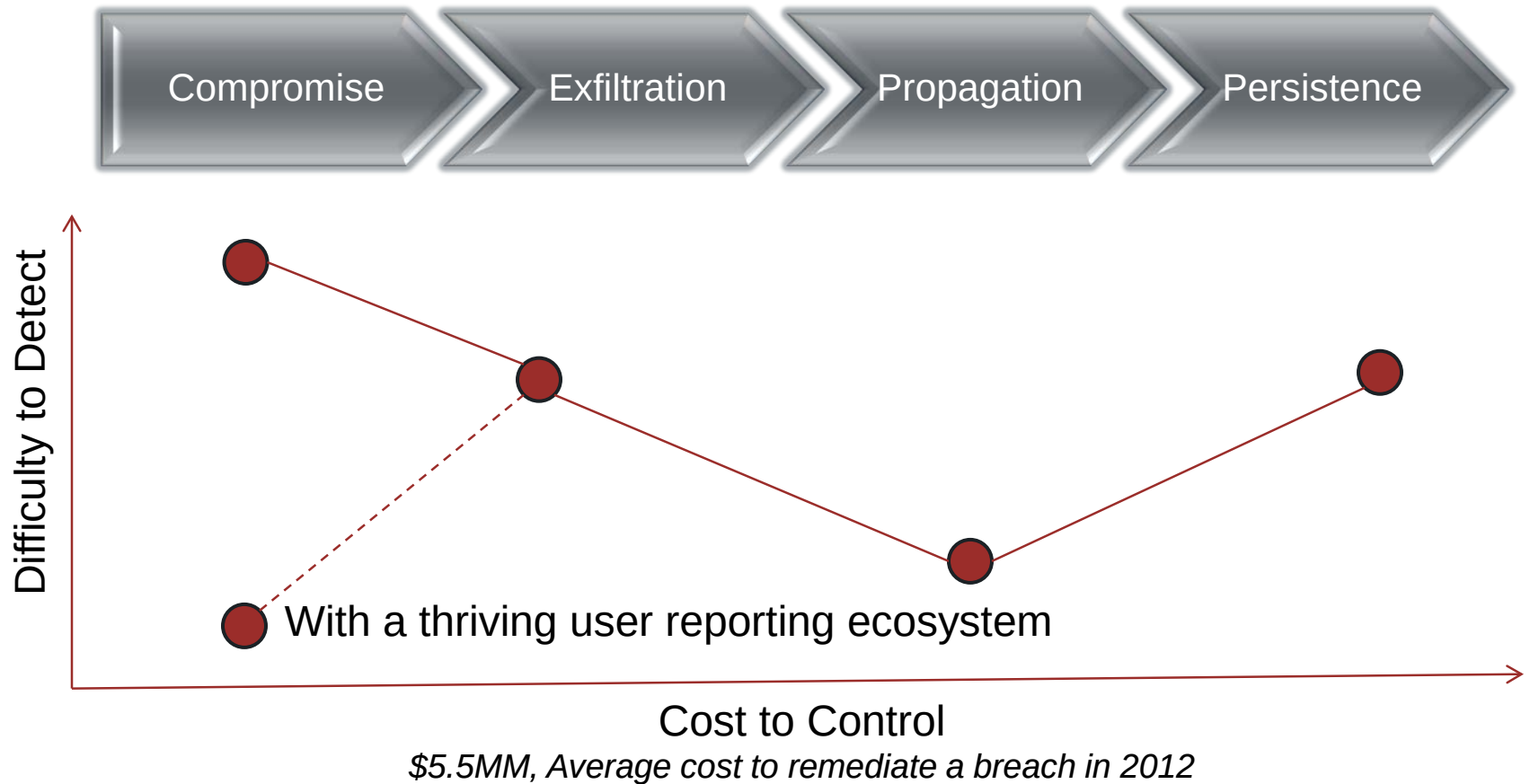
Can We Think Outside the Shiny Box?

Most people respond to emails within the first few hours of receiving them – if they are trained to report we get relevant, near time threat intelligence

Users who learn to not fall for phishing attacks also learn to report them



Control cost by incident phase



This is the end goal...



Conclusion

